Cybersecurity in healthcare

Given the increasing prevalence of cyber-attacks and the potential impacts to our systems and information, it is no surprise that cybersecurity is top of mind for CIO's. It is a key area of risk for senior teams and their Boards to manage.

Below is an excerpt from the 2019 HIMSS Cyber-security Survey Final Report:

> The 2019 HIMSS Cybersecurity Survey provides insight into the information security experiences and practices of US healthcare organizations in light of increasing cyber-attacks and compromises. Reflecting the feedback from 166 US-based health information security professionals, the findings of this study distill as follows:
>
> - A pattern of cyber-security threats and experiences is discernable across US healthcare organizations o
> - Significant security incidents are a near universal experience in US healthcare organizations with many of the incidents initiated by bad actors, leveraging e-mail as a means to compromise the integrity of their targets.
> - Many positive advances are occurring in healthcare cyber-security practices
> - Healthcare organizations appear to be allocating more of their information technology budgets to cyber-security.
> - Complacency with cyber-security practices can put cyber-security programs at risk.
> - There are certain responses that are not necessarily "bad" cyber-security practices, but may be an "early warning signal" about potential complacency seeping into the organization's information security practices.
> - Notable cyber-security gaps exist in key areas of the healthcare ecosystem
> - The lack of phishing tests in certain organizations and the pervasiveness of legacy systems raise grave concerns regarding the vulnerability of the healthcare ecosystem.

In light of these cybersecurity findings and risks, what are your thoughts on the following?

1. What is your organization doing to ensure the appropriate level of security is in place?
2. Do you feel your organization has appropriate experts with the right skillset and experience to navigate cybersecurity?
3. Should government provide a standardized cyber-security framework to follow?
4. Should government provide funding for cyber-security plans?
5. Is there opportunity for a regional approach to cyber-security?

HIMSS ON – About Us

HIMSS is a global advisor and thought leader supporting the transformation of health through information and technology. As a mission driven non-profit, HIMSS offers a unique depth and breadth of expertise in health innovation, public policy, workforce development, research and analytics to advise global leaders, stakeholders and influencers on best practices in health information and technology.

HIMSS ONTARIO Chapter

Chapters represent the grassroots of HIMSS. The Ontario Chapter of HIMSS is one of over fifty affiliated chapters of HIMSS and is the largest in Canada. Our purpose is to engage the Ontario healthcare system through global thinking and local leadership to create the bridge between technology and clinical outcomes for improved quality for patients, providers and institutions.

Visit the website to find out more, register as a member, and for more information on how to get involved including participation in various local sub-committees that support the Board chapter mandates.